Pembrokeshire County Council

Trading Standards

Avoiding Scams

www.pembrokeshire.gov.uk

Avoiding Scams

If you would like a copy of this leaflet
in large print, Braille, audio tape
or an alternative language, please contact
Pembrokeshire County Council
TSConsumer@pembrokeshire.gov.uk

Avoiding Scams

Avoiding Scams

Each year many people fall victim to fraudsters, intent on stealing their personal and financial information and conning them out of their cash. The fraudsters sound convincing, professional and may claim to represent a business you know, such as your bank. They may pressurise you to act quickly, either because they want to trick you into believing you will miss a golden opportunity to make money or that you will suffer some sort of loss if you fail to act. It only takes a single response to be inundated with many different scams as the scammers sell on your details.

If you are the victim of a scam it is important to seek support. Speak to someone you trust. Never stay silent.

Different types of scams

Five different types of scam are outlined in this leaflet:

1. Mail scams
2. Telephone scams
3. Text message scams
4. Internet and Social Media scams
5. Doorstep scams

Avoiding Scams

1. Mail Scams

- Letters are mass produced and made to look like personal letters or important documents. The intention is to trick you into giving your personal information, bank details or to send cash or make a money transfer.

Examples of Mail Scams

Lottery and Prize Draw Scams

- You are told that you have won a large cash prize in a lottery but you must send a fee in order to claim it.
- You have won a prize draw but must either phone a premium rate number or make an online purchase to claim it.

Clairvoyant and Miracle Cure scams

- Letters are sent promising a fortune reading for a fee.
- ‘Miracle’ cure scams promise quick and easy remedies for serious conditions or miraculous weight loss solutions. In some cases, a product is supplied that may actually damage your health.

Avoiding Scams

Remember…

- If it sounds too good to be true, it probably is.
- You cannot win a lottery or prize draw that you haven't entered.
- Be aware that scammers may already know information about the people they target.
- Be wary of catalogues and brochures selling over priced goods or insisting you place an order to be entered in a prize draw.

How to protect yourself…

- Never give out your personal details – shred unwanted documents with your personal details on.
- Never send money to claim prizes.
- Never buy any medicines or treatments without seeking advice from a healthcare professional.
- When registering to vote, tick the box to opt out of the 'Edited' register to prevent unsolicited marketing mail.
- Sign up for the Mail Preference Service to help reduce marketing letters. Call 0845 703 4599 or register online at www.mpsonline.org.uk.
- Subscribe to the Fund Raising Preference Service to end direct marketing contact from charities. Call 0300 3033517 or register online at www.fundraisingpreference.org.uk.
- To stop unwanted catalogues contact the business directly and ask to be removed from their mailing list. Legally they must do this.

Avoiding Scams

2. Telephone Scams

Examples of Telephone Scams

Computer software Scams

- A caller claiming to be from an official source tells you there is a problem or a virus on your computer. You are told to log into a website, but if you do, it will give the caller control over your computer, and access to your personal details.

Bank Scams

- You are told there are suspicious transactions on your account and you need to transfer it to another account. You may be asked to phone the number on the back of your bank card to legitimise the call but the scammer is still connected and pretends to be your bank answering the call. Your money is transferred to the scammer's bank account.

Amazon Scams

- You receive an automated phone call saying you have opened an Amazon Prime account and to press "1" on your phone if you want to cancel a transaction. If you press 1 the call connects to a fraudster posing as Amazon customer services, seeking access to your computer to resolve it. Your personal information including passwords and bank account details are stolen.
- Similar versions occur online claiming you have started a subscription or made a purchase.
- Amazon will never ask you for personal information, to make payment outside its website or to access your device.

Avoiding Scams

TV Licensing Scams

- New tv licensing requirements came in to effect in August 2020, resulting in less people being eligible for a free tv licence. Scammers have taken advantage, contacting consumers by phone, text or email claiming they need to make an urgent payment, are entitled to a refund or a cheaper licence.
- If you are unsure about a phonecall, do not provide personal details. For more details and advice go to www.tvlicensing.co.uk or phone 0300 555 0286.

Pension & Investment Scams

- Lifetime savings can be quickly lost to scammers, following contact out of the blue by phone, email, social media, letter or text. They may have convincing fake social media profiles or websites with fake reviews. They obtain details of investors on publicly available shareholder lists. There will usually be pressure to invest quickly or returns that sound too good to be true.
- In the UK a firm must be authorised and regulated by the Financial Conduct Authority (FCA) to do most financial services activities. If you use an unauthorised firm, you won't have access to the Financial Ombudsman Service (FOS) or Financial Services Compensation Scheme so you're unlikely to get your money back if things go wrong.
- Common investment scams include offers to buy or sell company shares, cryptocurrency (eg bitcoin), land banking, overseas property, binary options, sustainable energy, precious metals and wine investments.
- Reject unsolicited investment offers and check the FCA Warning List. Seek independent financial advice and make sure any firm you deal with is regulated by the FCA. Report concerns to the FCA on 0800 111 6768.

Avoiding Scams

- Common pension scams include early pension release and pension reviews. There are huge tax implications on withdrawing money from pensions before the age of 55. Pension cold calls are now banned. Report them to the Information Commissioner Office online at www.ico.org.uk or phone on 0303 123 1113.

Unpaid bills or refunds

- A caller phones and claims you have an overdue bill that needs paying immediately otherwise the service will be disconnected and you may be prosecuted. Examples include telephone, broadband providersand utility companies.
- A caller pretends you have overpaid for a service and are due a refund. You are asked to provide your bank details to transfer the money but instead money is taken out. A common example is scammers claiming to be HMRC.

Spoofing

- Criminals can “spoof” or mimic numbers of businesses to make it look like a legitimate call or text message or even a local number.

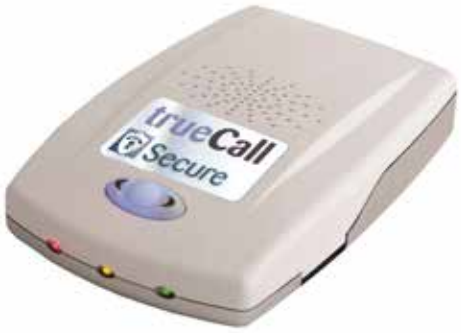
Authorised Push Payments

- Fraudsters may pressurise you to make immediate bank transfer or authorised push payments.
- If you’ve been tricked to make such a payment, contact your bank or card provider immediately to see if the payment can be stopped or if you can recover money from the fraudster’s account. Many high street banks have signed up to a voluntary Code which protects some victims that have lost money.

Avoiding Scams

How to protect yourself…

- Never give out your personal details or bank details over the phone unless you made the call and the phone number came from a trusted source.
- Ask for the name of the person calling and verify by contacting the company yourself using contact details you have established and not those provided by the caller. Always wait at least ten minutes before phoning to ensure the line is clear.
- Register with the Telephone Preference Service (TPS) for free to help reduce unsolicited calls. Call 0345 070 0707 or register online at www.tpsonline.org.uk.
- Report them to the Information Commissioner Office online at www.ico.org.uk or phone 0303 123 1113.
- Speak to your phone line provider to see if they provide services to stop or reduce unwanted calls.
- Consider purchasing a nuisance phone call blocking device.



- Pembrokeshire Trading Standards has a small number of ‘Truecall’ call blocking devices available for a trial period by vulnerable consumers who are experiencing problems with nuisance calls. Please contact the team for more details – email TSConsumer@pembrokeshire.gov.uk.

Avoiding Scams

3. Text Messages

SPAM and ScamTexts

- It can be difficult to tell the difference between a legitimate company and an attempted scam.
- Legitimate texts make it clear who is sending the text.
- Spam texts include those you have not consented to receive and usually try to persuade you to contact them regarding an accident claim, free holiday or medical claim, to obtain personal details.

  For details of how to stop and report unwanted texts contact the Information Commissioner Office (ICO) at www.ico.org.uk or phone 0303 123 1113.

Premium Rate Text Messages

- Businesses can legitimately send and charge for texts that you have signed up to receive. They are usually subscriptions for games and weather updates. They are costly and you may not know until you receive your phone bill.
- Check the small print before you sign up to a text service.
- Phone-paid Services Authority is the regulator of premium rate texts. For details of how to stop and report these messages visit www.psauthority.org.uk or phone 0300 30 300 20.

Avoiding Scams

4. Internet & Social Media Scam

- Many people prefer the convenience of shopping online for goods and services or keeping in touch through social networking sites such as Facebook, Instagram, twitter etc.
- They also provide a platform for scams in many forms including emails, pop-ups, social media messages and bogus websites.

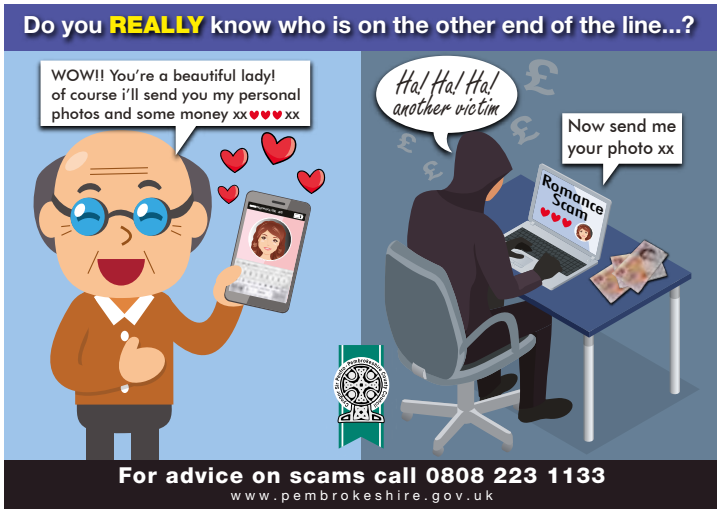
Examples of internet scams

Subscription Trap Scams

- You sign up online to a free trial or heavily discounted offer often for health or beauty products, forget to cancel it and find you are locked in a contract. Hidden in the terms is a continuous payment authority, allowing the business to take money from your account whenever it wants.

Romance Scams

- Fraudsters set up a fake profile on a dating or social media platform and strike up a conversation rapidly leading to an online relationship. They persuade you to chat away from the protection of the dating site messaging service.



- They often claim to work abroad and make excuses why they can't meet you.

Avoiding Scams

- When they think they have gained your trust they ask for money claiming for example they can't access their money to pay for a flight to see you or they have a present for you but you need to send them money to post it. This continues and the amounts requested increase with some victims selling their home and spiralling in to debt.
- Never give away too much information when dating online. Stay on the site's messaging service. Remember genuine people are unlikely to ask for money to help out with a problem.
- Often linked with romance scams is sexting or sextortion - the distribution or threatened distribution of nude or compromising images without the consent of the victim.
- Never pay out money otherwise the demands will continue. Stop communicating with the other person immediately and contact the police on 101. Detailed advice can be found online at www.nationalcrimeagency.gov.uk.

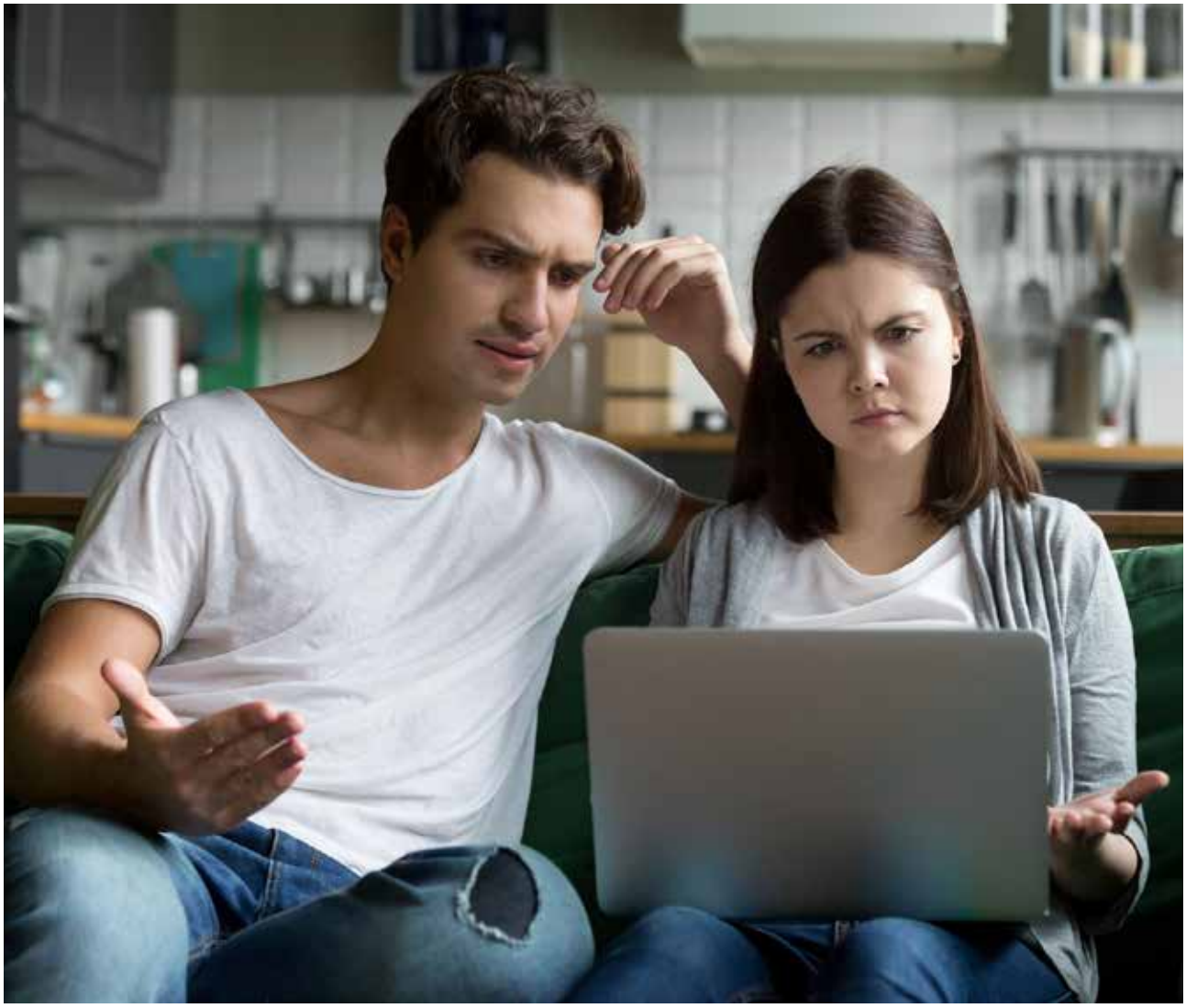
BitCoin Cryptocurrency

- Cryptocurrencies are unregulated virtual currencies that are used online. They allow you to pay for or make purchases rapidly and anonymously, making them attractive to scammers. Bitcoin is the most well known cryptocurrency. Scams increasingly demand payment in this format.

Avoiding Scams

Spam and Phishing emails

- Spam or junk emails are unsolicited and usually sent for marketing purposes. They may also contain scams, attempting to defraud you.
- Phishing emails appear to be from a legitimate source such as your bank, HMRC, an online shop or a networking site. The message attempts to deceive you in to providing personal and financial information and may direct you to a fake website or ask you to open an attachment that may contain a virus. Often the emails are written in an urgent tone and may have spelling mistakes.



Avoiding Scams

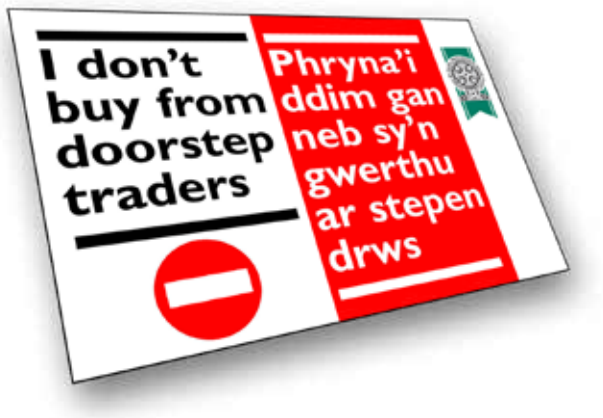
How to protect yourself…

- Ensure that you have up-to-date antivirus software and a firewall installed on your computer.
- Use strong passwords.
- When shopping online ensure the online link is secure – look for the padlock symbol in the browser and the web address begins with “https://”. The “s” is for secure. Don’t go off the platform to pay. Pay by credit card for purchases over £100, and research the business you are buying from.
- On social media sites keep your profile private and only accessible to family & friends. Be wary of publishing personal information about yourself that could identify you or where you live.
- Public wifi may not be secure and fraudsters could access and intercept what you are doing online so don’t send or receive private information or bank details.
- Do not open or reply to suspicious e-mails or open any attachments. Forward them to the National Cyber Security Centre at report@phishing.gov.uk who will take it down if it is a scam.
- Be wary of ‘pop-up’s’ and ‘free trials’ – as they are often associated with expensive charges.
- Look out for pre-ticked boxes which may commit you to more than you expect.
- Report unexpected payments to your bank.Legitimate banks and financial institutions will NEVER ask you to click on a link in an e-mail to access your account and will NEVER ask you for your PIN number.
- Visit www.getsafeonline.org for practical advice on how to protect yourself online.

Avoiding Scams

5. Doorstep Rogue Traders

- Doorstep rogue traders cold call selling goods or services that are poor quality, unnecessary or very expensive. Typically gardening and home maintenance services are offered.
- They pressurise the resident to make a quick decision claiming the offer is only valid that day or that there is a risk of danger if the work is not completed immediately.
- Often there is no upfront paperwork detailing the work or price agreed and the price often increases after the work has begun.
- Traders can become aggressive and intimidating.
- Some rogue traders pose as officials or conduct surveys to obtain your personal details and disguise their real intent.



How to protect yourself…

- Display a 'I don't buy from doorstep traders' sticker on your door. These can be obtained from Pembrokeshire County Council Trading Standards Team.
- Don't buy goods or services from cold callers.
- If you need work carried out, ask family or friends to recommend traders and obtain a number of written quotes before deciding.
- Never let anyone in your house unless they are someone you know and trust.
- If a trader becomes aggressive or makes you feel intimidated and they are at your property or due to return, phone the police on 101.

Avoiding Scams

Green Energy Schemes ...

- There are many legitimate government funded schemes aimed at improving home energy efficiency offering for example new boilers, home insulation or alternative energy devices such as solar panels or air source heat pumps.
- Agents and businesses offering the schemes may cold call by phone or in person to see if you are eligible.
- If you are interested in the scheme carry out your own research before agreeing any work to see if it's suitable. Verify if the Council is aware of the business.

If you have been targeted by a scam or you are concerned that a relative, friend or neighbour may have been targeted by a scam contact:

Citizens Advice Consumer Service on 0808 223 1133 for advice

The information is shared with Pembrokeshire County Council Trading Standards team, who may get in touch